IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF NEW MEXICO

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	CRIMINAL NO. 15-4268 JB
	)	
ANGEL DELEON, et al.,	)	
	)	
Defendants.	)	

UNITED STATES' OPPOSED MOTION TO RECONSIDER THE COURT'S ORDER FOR LIMITED PRODUCTION OF SENSITIVE GOVERNMENT RECORDING DEVICES OR PROGRAMS

On November 27, 2017, this Court ordered the United States to allow one Defendant's attorney and that attorney's computer forensic examiner to inspect one of the sensitive government recording devices -- referred to as an ELSUR recording device.[1] The Court ordered this production under the theory that, because these devices were given to cooperating human sources ("CHSs"), whom have criminal history, the Court could not conclude, logically, "[w]hat is so secret now [about the ELSUR device] that we're in a court that I can't have one lawyer and one expert look at it?" November 9, 2017 Motions Hearing Transcript ("Tr.") at 17:2-9 (Court).

But the United States did not properly assert the law-enforcement-sensitive qualified evidentiary privilege. So the Court ordered this production without making the findings and conclusions that are necessary and proper to overcome the law-enforcement-sensitive qualified privilege. Plus, at the time the Court ordered this limited production, the United States didn't understand fully the operation of the ELSUR device. So the United States didn't provide the

[1] ELSUR is an acronym used by the FBI to abbreviate "Electronic Surveillance."

Court with a sufficient factual background on which the Court may analyze the Defendants' request for production of the ELSUR device. With the proper background, the Court will conclude that production, even in the limited nature in which the Court ordered it, would not lead to discovery of any useful information, and may serve only to harm national security interests.

Because of these deficiencies in the record and the incorrect assumptions on which the Court ordered production, for which the United States is responsible, the United States moves the Court to reconsider its order. The United States asks that, in support of this motion, the Court allow the United States to present testimony from FBI Operational Technology Division Supervisory Special Agent Hugh S. Williamson, Program Manager for the FBI Body Recorder Program. At the conclusion of Sup. SA Williamson's testimony, the Court may conclude properly that there is no sound basis on which the Defendants may discover further information about the ELSUR device, and that, regardless, the Defendants cannot overcome the law-enforcement-sensitive qualified evidentiary privilege.

Pursuant to D.N.M.LR-Cr. 47.1, the United States sought concurrence of Defendants. Defendants oppose this motion to reconsider.

BACKGROUND

A. FACTUAL BACKGROUND

The United States began the investigation into the SNM prison gang that led to this prosecution on or about March of 2015. Because the SNM prison gang operates primarily within the confines of the prison, and because of the difficult nature of penetrating this criminal organization, the FBI used CHSs to record incriminating conversations with the Defendants. In that process, the FBI provided the CHSs with covert ELSUR devices to record the conversations.

The ELSUR devices used in this case were Hawk 3A devices, which are manufactured by Adaptive Digital Systems, Inc. ("ADS"). The Hawk 3A device is an audio-only body recorder. These Hawk devices incorporate a multi-layer protection system to ensure the integrity of the evidence collected by the recording, which system includes data integrity protection during the recording and after the data is downloaded. *See* ADS BODY RECORDER, DATA HANDLING/PROTECTION, executed by Attila W. Mathe, ADS President, October 17, 2017 (Attached as Ex. A) ("Mathe ADS Declaration").

The operator of the Hawk device -- the CHSs here -- may turn "OFF" and "ON" the device. Each time that the device is turned on and then off, "a new session is created." *Id.* As Attila W. Mathe, ADS President, explains (and as Sup. SA Williamson will testify), snippets of recordings taken by the device operator during a conversation are apparent from the metadata and from the Bird software when playing the recording:[2]

> Any attempt to manipulate the recording by turning the device off and on in the middle of a conversation would generate a separate recording session and would be apparent in the metadata generated by the device and on the computer screen when the user downloads the data containing the recordings. As a result the fact that a recording has only one session means that the recording device ran continuously, without interruption, throughout the conversation.

Mathe ADS Declaration.

Aside from separate recordings made by the user turning "ON" and "OFF" the devices, the devices themselves may create separate recording files when the data from a recording is too

[2] The Bird software is the ADS software that is used to play the recordings and view the metadata about the recordings. It is a proprietary software created, maintained and serviced by ADS. *See* Mathe ADS Declaration. The Court witnessed the Bird software's operation during the November 27, 2017 motions hearing. The Bird software was included in the production of the ELSUR device metadata when the evidentiary optical drive discs (DVDs) were produced to Defendants in June 2017. The Bird software is the only medium through which the Hawk device recordings may be played. The FBI does not maintain or edit the Bird software; it only receives updates of the software from ADS.

large for one file. When this happens, there is a flag that appears on the Bird software to alert the person viewing the Bird software and playing the recording that separate files were created because of the file size. Also, separate recordings may occur because of a problem in the device. For instance, the battery may run out or otherwise malfunction (*i.e.*, the recording ended because the battery malfunctioned, and not because the user switched the recording to "OFF"). If this happens, a flag appears on the Bird software to alert the person viewing the Bird software and playing the recording that separate files were created because of a battery malfunction. If the device is turned "ON" and the user does not then turn the device "OFF", it will continue recording until it runs out of power or runs out of memory.

The Hawk devices cannot play the recordings or otherwise retrieve the recordings; they can only receive audio one way. The only way in which to listen to the recordings/review the data on the Hawk device is to download -- through ADS proprietary software -- the data to an optical disc or drive and then play the recording sessions through the Bird software. The Hawk device user, the CHSs, aren't able to manipulate the data on the device or record over the data.

All of the data on the Hawk recording devices is downloaded to an evidentiary optical drive or disc -- in this case, optical disc DVDs -- by the FBI ELSUR Operations Technician in Albuquerque, New Mexico. The data is downloaded on a standalone computer which is devoted solely to downloading ELSUR devices. The data from the Hawk devices is not stored on that computer; it is downloaded directly to the particular evidentiary optical drive or disc. Only the ELSUR Operations Technician accesses the computer that downloads the data from the ELSUR devices; case agents or other technical agents aren't allowed access. The standalone computer and ADS proprietary software ensures that all of the data is transferred to the evidentiary optical drive or disk. When all of the data from the ELSUR device is transferred to the evidentiary

optical drive or disc, then the ADS software erases the data on the ELSUR device so that it may be re-deployed in the field. If there is a problem with the download, the ADS software alerts the Operations Technician to that problem and will not allow the ELSUR, in this case, Hawk, device to be erased. If that happens, the device is sent to the FBI Operational Technology Division ("OTD") in Quantico, Virginia. If the ELSUR device cannot be fully downloaded at OTD without issue, then the device is provided to ADS to assess the problem and/or download all of the data from the device.

While the Hawk device is recording, it creates authentication hashing; it's a numerical coding on the device's internal computer. When the data on the Hawk device is transferred to the optical drive or disk by the ELSUR Operations Technician, the original authentication hashing is maintained with the data. The ADS software generates a hash value based on an algorithm for every 512 MB of data. When using the Bird software to playback the recordings, the data (and hashing) is checked by the Bird software, and will only play the recordings if the authentication hash matches. "If an error is detected a 'CHECKSUM ERROR' message is displayed on the computer screen and the recording will not play. Any alteration to the data would be detected on this check." Mathe ADS Declaration.

The United States provided to Defendants in June 2017 the evidentiary DVDs that contain the ELSUR information from the Hawk recording devices, including the recordings, the metadata, and the Bird software which allows the recordings to play on a computer. The data on the Hawk devices was downloaded to the evidentiary DVDs by the ELSUR Operations Technician without problem. This means that the information on the Hawk devices was erased, and the information on them exists only on the evidentiary DVDs provided to Defendants.

B. PROCEDURAL BACKGROUND

1. Defendant Daniel Sanchez's Motion to Compel Specific Discovery [Doc. 1253].

On September 15, 2017, Defendant Daniel Sanchez filed his Motion to Compel Specific Discovery [Doc. 1253] ("Sanchez MTC"). In Paragraph J of the Sanchez MTC, Sanchez provides the background for his request for "access to the ELSUR devices for purpose of examining the metadata stored on them." *Id.* ¶ J, at 12-13. Sanchez appears to base his request for access to the ELSUR devices on Rule 16(a)(1)(E). *See id.* at 13. He contends that the Court should allow him access to the devices "to determine whether recordings have been altered or deleted or whether additional recordings exist that have not been disclosed." *Id.* He further contends that "[t]his meta data will also assist in determining the time and length of the recordings and the order in which they were created." *Id.*

2. United States' Response to Defendant Daniel Sanchez's Motion to Compel Specific Discovery [Doc. 1282] ("Sanchez MTC Response").

The United States objected to Sanchez's request to access the ELSUR devices, because his "request fails to find support under the law enforcement privilege and constitutes an impermissible fishing expedition." Sanchez MTC Response at 8 (citing *Mohammed v. Holder*, 2014 U.S. Dist. LEXIS 35297, at *12-13 (D. Colo. Mar. 17, 2014)). The United States pointed out the dangerous consequences of allowing Sanchez access to the ELSUR devices, including the possible counterintelligence use to which that information may be put. *See id.* at 8-9 (citing *United States v. Rodella*, 2015 U.S. Dist. LEXIS 20704, at *65-66 (D.N.M. 2015) (Browning, J.) (citing *United States v. Mayes*, 917 F.3d 457, 461 (10th Cir. 1990)). The United States asserted that, in the absence of evidence that the recordings do not fairly and accurately represent the statements made to the CHSs, "Defendant should not be permitted to embark on a fishing

expedition of the Government's means and methods of investigation to search for any evidence that could conceivably benefit Defendant." *Id.* at 9.

3. November 9, 2017 Motions Hearing on Sanchez's MTC.

At the hearing on Sanchez's MTC, in discussion of the ELSUR devices, the United States informed the Court that "there is no information on the devices anymore for inspection." Tr. at 5:2-5 (Castellano). The United States asserted that, an agent checks out device and deploys it to the user, in this case, the CHS. The United States asserted that "[t]he device only is on or off. So there is no ability, even by the agent, to delete information from the device. So an informant or the agent can't delete. It's either recording or it's not recording." *Id.* at 5:7-11 (Castellano). The United States stated: "Once the device is finished, the agent returns it to the -- whoever maintains the devices. The device is downloaded, and the device is redeployed into the field for use. So the information is basically deleted or recorded over. So there is no information to get from the devices." *Id.* at 5:11-17 (Castellano).

After some discussion with the United States, the Court asked whether these Hawk devices possess "like a hard drive on these devices that record on." *Id.* at 13-14 (Court). The Court was correct; the Hawk devices have an internal solid-state hard drive that maintains the data when they're deployed in the field. But the United States didn't know that at the time. *See id.* at 6: 15-17. The United States told the Court that it was correct that the field agents "hand [the Haw device] to somebody and they get the information off of it." *Id.* at 6:18-22 (Court, Castellano). The United States informed the Court that it was also correct that "all the devices right now are, for lack of a better word, just empty." Tr. at 6:23-7:2 (Court, Castellano).

At that point in the hearing, the United States used a copy of the evidentiary DVD which Defendants possess to demonstrate the ADS Bird software, which demonstrates the ability to

play the recordings on a computer and view the metadata about the recordings that the Hawk device captures. *See id.* at 7:3-8:21 (Castellano).

The Court discussed with the United States the metadata that the Bird software displayed. The Court asked about the first recording session on the DVD and noticed that the Bird software showed "a six-second gap [after the first session] before we go to the second [session]." *Id.* at 8:22-9:3 (Castellano). The United States responded that, "[i]f the time stamp is correct, yes, it looks like there is approximately a six-second gap; the recording stops; there is a six-second gap; then an 18-second recording [session]." *Id.* at 9:4-7 (Castellano). The Court then asked the United States whether the Bird software shows that there 19 minutes passed between the second and third session, to which the United States agreed. *See id.* at 9:8-10:20 (Court, Castellano).

Regarding the gaps between the sessions, the United States failed to provide the necessary information to the Court and the Defendants what may cause the gaps between the recording sessions. The Court asked: "We've got a couple of gaps. What causes the gaps? What is the -- why do gaps exist?" *Id.* at 10:21-23 (Court). The United States responded that, at that time, it didn't know: "I don't know, Your Honor. I don't know the technology. Or if that's a start and stop function. So my guess, which I think is going to be pretty close, is either there is a problem with the technology, or it's a start and stop by the person using it." Tr. at 10:24-11:4 (Castellano). At the Court's questioning, the United States stated that it's the United States' understanding that "the only thing the person [that's got the recording device] can do is either have it on and recording, or off. There is no deletion or anything else." *Id.* at 11:5-11 (Court, Castellano). The United States confirmed it's understanding that the CHS "just has an on and off button." *Id.* at 11:12-14 (Court, Castellano).

The United States and the Court discussed whether the United States was willing to disclose the type of device so that the defense could obtain a prototype and look at it, to which the United States responded that it anticipated that the FBI would not disclose that information. *See id.* at 12:5-16 (Court, Castellano).[3]

The Court then heard from Sanchez. Sanchez analogized the Hawk device's computer system to a personal computer, contending that, whereas deleting a word-processing file from a computer doesn't delete the metadata, the "electronic remnant of that file" on the Hawk devices' computer "remains." *Id.* at 13:11-23 (Jacks). The Court pointed out that those files may remain on the device, but they "may be somewhere in Washington or at the FBI headquarters, right?" *Id.* at 13:24-14:2 (Court). To which Sanchez responded that he doesn't know what was done to the device, and a forensic computer expert may find electronic data on the device. *See* Tr. at 14:4-13 (Jacks).[4] Sanchez contended that, what the United States showed to the Court, was "what the software program can access. But that doesn't mean that there weren't other files that were deleted before those files were downloaded." *Id.* 14:14-17 (Jacks).[5] Sanchez stated that the defense would prefer access to a similar device to verify the United States' representations. *See id.* at 14:18-23 (Jacks). Sanchez asserted that he and the other defendants "first . . . have to be

[3] The type of device used was an ADS Hawk 3A device.

[4] The United States anticipates that Sup. SA Williamson will testify that the data does not remain on the devices, nor does it reside in Washington or at FBI headquarters. All of the data that was on the Hawk devices used in this case was downloaded onto the evidentiary DVDs in the Albuquerque FBI office by the ELSUR Operations Technician, which DVDs were provided to the discovery coordinator and, thus, to Defendants.

[5] It's correct that the Bird software played in Court was what the Bird software can access. But contained on each evidentiary DVD is all of the information that was downloaded off of that particular Hawk device. As Sup. SA Williamson will explain, that the evidentiary DVD was created at all, and did not produce a "'CHECKSUM ERROR'" when downloaded by the ELSUR Operations Technician, Mathe ADS Declaration, establishes that "there weren't other files that were deleted before those files were downloaded." Tr. at 14:15-17 (Jacks).

able to understand, what electronic data, if any, did the Government destroy by wiping the devices or not preserving the devices for inspection by the defense." *Id.* at 15:5-8 (Jacks).[6]

The Court ordered the Defendants to ask questions of the United States about the recording devices, *see id.* at 15:9-15 (Court), which the Defendants did, *see* Notice of Letter to Government Regarding Questions about Electronic Surveillance [Doc. 1459], and to which the United States responded, *See* United States' Response to the Notice [Doc. 1548]. The Court noted that the Defendants had close to enough information about the devices, but there was still an outstanding issue about how to account for the gaps in the recording sessions. *See* Tr. at 15:16-23 (Court).

Sanchez responded with criticism that

> the Government makes this big deal about we can't tell a defense lawyer what the device was, but they gave these devices to people that have been convicted of murder and all sorts of heinous offenses to possess in their cell, in prison, with absolutely no supervision. So I'm not understanding what is lost by allowing a defense lawyer and a defense expert to have access to the device to try to determine what has been deleted from it.

Id. at 15:25-16:10 (Jacks). Sanchez asserted that there was a problem with the United States having provided these devices to CHS "to possess in their cell for some lengthy period of time, where they're free to . . . do whatever they want to it," and that there has now been "absolutely no effort made . . . here" to make sure that the CHSs used the device in a proper, reliable manner.[7] *Id.* at 16:11-17:1 (Jacks).

[6] Sup. SA Williamson's testimony will clarify that the creation of the evidentiary DVDs ensures that no data is destroyed or lost by wiping the Hawk devices; production of the DVDs in this case is possible only if the data integrity systems find that the original data is not altered in any way and is downloaded fully.

[7] The United States anticipates that Sup. SA Williamson will explain during his testimony that the multi-layer protection system that is incorporated into these Hawk devices and software, including the authentication hash values, the hash value based on the ADS algorithm, and the

The Court concluded that it would "push" the United States for more information, and acknowledged that Sanchez's argument "has some force." *Id.* at 17:2-10 (Court). The Court cautioned, "[b]ut I'm not quite convinced that, A, it's going to produce anything, other than what you've got. I'm also not convicted that it's the most secretive thing in the world." *Id.* at 17:9-14 (Court).[8]

4. Motion Hearing and Order to Produce on November 27, 2017.

At the motions hearing that this Court held on November 27, 2017, Sanchez and the other Defendants re-raised the issue about the ELSUR recording devices.[9] The Court inquired whether the United States answered Defendants' questions about the devices, or otherwise received more information about the FBI's non-disclosure, to which the United States responded that it had not. *See* November 27, 2017 Hearing Transcript ("Nov. 27 Tr.") at 140:8-21 (Court, Beck). The Court asked whether ordering the limited production of a Hawk device to one Defendant's attorney and that Defendant's attorney's forensic computer expert would "move" resolution of the issue "forward." *Id.* at 140:22 (Court). The Court acknowledged that it may be willing to consider a motion to reconsider the order under this proposed order: "I mean if I ordered it, and then with the understanding the Government could come back and ask me to reconsider before anything is done, would that move things forward so we can get a final answer from the FBI?" *Id.* at 140:23-141:2 (Court). The United States agreed that an oral order of limited production

---

hash verifications when the data is downloaded from the Hawk devices, ensures that the CHSs used the device in a proper, reliable manner, and that the data wasn't manipulated in any way.

[8] Indeed, allowing an attorney and a forensic computer expert to access the Hawk devices will not produce anything probative other than what the Defendants already possess. It will produce only the opportunity to develop counterintelligence about the Hawk device, which serves only to harm national security interests.

[9] The United States doesn't yet possess the transcript from this motions hearing.

would help expedite a resolution. The Court, therefore, ordered the limited production. *See id.* at 141:11 (Court).

On November 29, 2017, the United States informed the Court that it had been in discussion with the FBI, and the United States intended to file a motion to reconsider the Court's order. The United States agreed to file this motion to reconsider on or before December 6, 2017. The United States represented at that time that it didn't intend to present any witnesses or other additional evidence.

On December 1, 2017, however, counsel for the United States attended a conference call with the FBI OTD. At that time, it was decided that the United States would present the testimony of Sup. SA Williamson to support this Motion to Reconsider. A copy of Sup. SA Williamson's CV is attached to this Motion to Reconsider as Ex. B, and two transcripts of his previous trial testimony about similar ELSUR devices, but not Hawk devices, are attached.

LAW REGARDING THE LAW-ENFORCEMENT-SENSTIVE QUALIFED EVIDENTIARY PRIVLEGE

A. THE LAW-ENFORCEMENT-SENSITIVE EVIDENTIARY PRIVILEGE

The Supreme Court in *Roviaro v. United States*, recognized an "informer's privilege" that protects the identity of government informants and allows the government to withhold from disclosure the identity of persons who furnish information of violations of law to officers charged with enforcement of that law. The purpose of the privilege is the furtherance and protection of the public interest in effective law enforcement. *Roviaro*, 353 U.S. 53, 59 (1957).

Courts extended the *Roviaro* privilege to cover other investigative techniques, including traditional and electronic surveillance. For example, in *United States v. Green*, the D.C. Circuit upheld the privilege over a defendant's request to learn the location of an observation post used in a drug investigation:

> Just as the disclosure of an informer's identity may destroy his future usefulness in criminal investigations, the identification of a hidden observation post will likely destroy the future value of that location for police surveillance. The revelation of a surveillance location might also threaten the safety of police officers using the observation post, or lead to adversity for cooperative owners or occupants of the building. Finally, the assurance of nondisclosure of a surveillance location may be necessary to encourage property owners or occupants to allow the police to make such use of their property.

United States v. Green, 670 F.2d 1148, 1155-1158 (D.C. Cir. 1981).

Courts have held that, given "the public interest in effective law enforcement," the FBI may assert a qualified privilege to protect sensitive law enforcement techniques and procedures from disclosure. *Roviaro*, 353 U.S. at 59. *See In re The City of New York*, 607 F.3d 923, 944 (2d Cir. 2010) ("'An investigation . . . need not be ongoing for the law enforcement privilege to apply as the ability of a law enforcement agency to conduct future investigations may be seriously impaired if certain information' is revealed to the public." (quoting *Nat'l Congress for P.R. Rights ex rel. Perez v. City of N.Y.*, 194 F.R.D. 88, 95 (S.D.N.Y.2000)); C*ommonwealth of Puerto Rico v. United States*, 490 F.3d 50, 62-64 (1st Cir. 2007). With respect to electronic surveillance equipment, the 11th Circuit has held that the privilege applies, if information about the equipment is provided to defendants and the public, and it will "educate criminals regarding how to protect themselves against police surveillance. Electronic surveillance is an important tool of law enforcement, and its effectiveness should not be unnecessarily compromised**.** Disclosure of such information will also educate persons on how to employ such techniques themselves, in violation of Title III." *United States v. Van Horn*, 789 F.2d 1492, 1508 (11th Cir 1986).

Even where some aspects of a protected technique are known to the public, "there is no principle . . . that requires an agency to release all details concerning these and similar techniques

simply because some aspects of them are known to the public." *Barnard v. U.S. Dep't of Homeland Security*, 598 F.Supp.2d 1, 23 (D.D.C. 2009). *See also Piper v. Dep't of Justice*, 294 F.Supp.2d 16, 31 (D.D.C. 2003) (in FOIA case, court accepted arguments that disclosure of the identity of an electronic device used for monitoring purposes would reduce its effectiveness and allow for individuals being investigated by the FBI to take countermeasures to circumvent the technique).

The law enforcement sensitive evidentiary privilege is "grounded in well-established doctrine and is widely recognized by the federal courts." *In re The City of New York*, 607 F.3d at 941 n.18. The privilege is designed to, among other things, prevent disclosure of law enforcement techniques and procedures that, once revealed, could risk future circumvention of the law or compromise of the technique. *See id*. at 944. *See also United States v. Winner*, 641 F.2d 825, 831 (10th Cir.1981) (stating that the "law enforcement investigative privilege is based primarily on the harm to law enforcement efforts which might arise from public disclosure of investigatory files") (internal quotation marks and ellipsis omitted); *Tuite v. Henry*, 181 F.R.D. 175, 176-77 (D.D.C. July 31, 1998) (unpublished), *aff'd*, 203 F.3d 53 (D.C. Cir. 1999) ("The federal law enforcement privilege is a qualified privilege designed to prevent disclosure of information that would be contrary to the public interest in the effective functioning of law enforcement. [It] serves to preserve the integrity of law enforcement techniques and confidential sources, protects witnesses and law enforcement personnel, safeguards the privacy of individuals under investigation, and prevents interference with investigations."); *Van Horn*, 789 F.2d at 1507-1508 (11th Cir. 1986) (finding the existence of a qualified government privilege not to disclose sensitive investigative techniques); *Dellwood Farms v. Cargill, Inc.*, 128 F.3d 1122, 1125 (7th Cir. 1997); *In re Dep't of Investigation*, 856 F.2d 481, 483-84 (2d Cir. 1988) (stating

that the law enforcement privilege exists and prevents the "disclosure of law enforcement techniques and procedures, [preserves] the confidentiality of sources, [protects] witnesses and law enforcement personnel, [safeguards] the privacy of individuals involved in an investigation, and otherwise [prevents] interference with an investigation"); *United States v. Harley*, 682 F.2d 1018, 1020-21 (D.C. Cir. 1982); *Green*, 670 F.2d at 1148.

Technical specifications to include the installation, concealment and location of audio recording devices installed in the defendant's apartment are covered by the "law enforcement sensitive" qualified evidentiary privilege. *See In re U.S. Dep't of Homeland Sec.*, 459 F.3d 565, 569-71 (5th Cir. 2006) (finding that "in today's times the compelled production of government documents could impact highly sensitive matters relating to national security. Therefore, the reasons for recognizing the law enforcement privilege are even more compelling now than when [prior cases in the 5th Circuit] were decided."); *Tuite*, 181 F.D.R. at 176-77.

In *Van Horn*, the Eleventh Circuit specifically recognized that the privilege applies to electronic surveillance devices and upheld the privilege over the defendant's request to learn the type and placement of microphones in a co-defendant's office. *See* 789 F.2d at 1507-08. As referred to above, the law enforcement privilege prevents disclosure, preserves the confidentiality of sources, protects law enforcement, maintains the privacy of individuals, and prevents interference with an investigation." *In re Dep't of Investigation*, 856 F.2d 481, 483-84 (2d Cir. 1988); *Winner*, 641 F.2d at 831 (10th Cir.1981) (stating the "law enforcement investigative privilege is based primarily on the harm to law enforcement efforts which might arise from public disclosure of investigatory files" (internal quotation marks and ellipsis omitted)); *see also Harley*, 682 F.2d at 1020-21; *Green*, 670 F.2d at 1148.

B. APPLICATION OF THE LAW-ENFORCEMENT-SENSITIVE QUALIFIED EVIDENTIARY PRIVILEGE.

The law enforcement privilege is a qualified, and not absolute, privilege. There are circumstances, therefore, in which information subject to the privilege must nevertheless be disclosed. *In re The City of New York*, 607 F.3d at 940. The Second Circuit has analyzed, in depth, the actual procedure that should be followed by a court in determining whether the privilege bars disclosure. *Id*. at 948-49.

As a threshold matter, the party that asserts the law-enforcement privilege bears the burden to demonstrate that the material is the type of material that the law-enforcement privilege is intended to protect -- in this case, information pertaining to law-enforcement techniques and procedures, as well as information that would seriously impair the ability of a law enforcement agency to conduct future investigations. *Id*. at 948.

Once the party asserting the privilege successfully shows that the law-enforcement privilege applies, "there ought to be a pretty strong presumption against lifting the privilege." *Id*. at 945 (quoting *Dellwood Farms*, 128 F.3d at 1125). The Court must balance the public interest in non-disclosure against the need of a particular litigant for access to the privileged information. *Id.* at 948 (quoting *In re Sealed Case*, 856 F.2d 268, 272 (D.C. Cir. 1988)); *see also Dellwood Farms*, 128 F.3d at 1125 (holding that the actual determination of the existence of the law enforcement sensitive privilege is a "particularistic and judgmental task" that involves balancing the "need of the litigant who is seeking privileged investigative materials . . . against the harm to the government if the privilege is lifted. . .").

To rebut the presumption against lifting the privilege, the party seeking disclosure must show: (1) the request is "non-frivolous and brought in good faith"; (2) "the information sought is [not] available through other discovery or from other sources"; and (3) there is a "compelling

need" for the information relevant to the party's case. *In re City of New York*, 607 F.3d at 948 (quoting *Friedman v. Bache Halsey Stuart Shields, Inc.*, 738 F. 2d 1336, 1343 (D.C. Cir. 1984)).[10] Even if the party seeking disclosure successfully rebuts the presumption (by a showing of, among other things, a "compelling need"), the Court must then continue the inquiry by weighing the public interest in non-disclosure against the need of the litigant for access to the privileged information before ultimately deciding whether disclosure is required. *In re City of New York*, 607 F.3d at 945.

To assess both the applicability of the privilege and the need for the materials, the Court must ordinarily review *ex parte* the materials in question or hold an evidentiary hearing in chambers. Frequently, because filing documents under seal may inadequately protect particularly sensitive information, the Court may, in the exercise of its informed discretion and on the basis of the circumstances presented, require that the party possessing the materials appear *ex parte* in chambers to submit the materials for in camera review by the judge. *Id.* at 948-49; *see id.* at 949 n.25 (an appropriately general docket entry memorializing any *ex parte* proceedings can be entered in the public records of the district court so long as it does not compromise the interests of the party holding the confidential information, or the public); *In re U.S. Department of Homeland Security*, 459 F.3d at 571 (instructing the district court to review the information for

[10] Courts have used other criteria to determining whether the party seeking disclosure has rebutted the law-enforcement privilege with respect to investigative equipment. These criteria may often be referred to as the *Frankenhauser* criteria. *Cf. Frankenhauser v. Rizzo*, 59 F.R.D. 339, 344 (E.D. Pa. 1973). These criteria include: whether the party seeking discovery is an actual or potential defendant in any criminal proceeding either pending or reasonably likely to follow from the incident in question; whether the investigation has been completed; whether the information sought is available through other discovery or from other sources; and the importance of the information sought to the plaintiff's case. *See id.*, 59 F.R.D. at 344; *Tuite*, 181 F.R.D. at 175; *In re Sealed Case*, 856 F.2d at 272.

which the law enforcement sensitive privilege is being asserted in camera to evaluate whether the privilege applies.)

If the Court determines that the law-enforcement privilege is not sufficient to protect disclosure of the materials at issue, the materials must be disclosed. *See In re The City of New York*, 607 F.3d at 949. To minimize the effects of disclosure, however, the Court can restrict the manner in which the materials are provided through the issuance of a protective order. The Second Circuit suggested that, where release is directed, the materials should be available only on an "attorneys' eyes only" basis, or requiring that the documents-and other submissions that reference them-be filed under seal. *See id.*

The court will essentially consider the defendant's "need [for] the evidence to conduct his defense and [whether] there are . . . adequate alternative means of getting at the same point. The degree of the handicap [to the defendant] must then be weighed by the trial judge against the policies underlying the privilege." *Harley*, 682 F.2d at 1020 (D.C. Cir. 1982); *see also United States v. Cintolo*, 818 F.2d 980, 1002 (1st Cir. 1987) (reviewing "whether the [defendant] demonstrate[s] an authentic 'necessity,' given the circumstances, to overbear the qualified privilege"); *United States v. Foster*, 986 F.2d 541, 543-45 (D.C. Cir. 1993) (balancing defendant's need for information against importance of government's interest in avoiding disclosure).

ARGUMENT

Before the Court ordered orally the production of an ELSUR device used in this case, the United States failed to develop the record in a manner sufficient for the Court to make an informed decision as to the basis of that order. The record was not clear that the CHS using the ELSUR recording device could turn "OFF" or "ON" the recording mechanism on the device

only. The record was not clear whether some data (or metadata) may remain on the ELSUR recording device after that data was downloaded to the evidentiary DVDs and the ELSUR recording device's computer was erased. The record was not clear even whether the evidentiary DVDs produced to Defendants contained all of the data (and metadata) that was contained on the ELSUR devices. Because of these deficiencies in the record, the Court could not reach the conclusion that allowing Defendants access to the ELSUR devices or a similar-type device would not produce nothing of any probative value in addition to what Defendants already have. But with submission of this motion to reconsider, and with the testimony of the FBI's OTD Body Recorder Program Manager, which the United States intends to present during the hearing on this motion, the Court will have a sound basis to reconsider its order of production and conclude that access to the devices is not warranted. The United States thus moves the Court to reconsider.

A. SANCHEZ SHOWS THAT RULE 16 ENTITLES HIM TO THE METADATA.

Reconsideration of the Court's Order, and resolution of the Defendants' request for access to the ELSUR recording devices -- the Hawk recording devices in this case -- may be quickly resolved if we go back to the Sanchez's original basis for his request in his Sanchez MTC. There, he provides a sound basis for discovery of material to which, under the circumstances, he has demonstrated Rule 16 entitles him. *See United States v. DeLeon*, No. CR 15-4268 JB, 2017 WL 2271430, at *48 (D.N.M. Feb. 8, 2017) (Browning, J) (concluding the Court will order production under Rule 16 only once a Defendant "make[s] the necessary showing" that the requested material fits under Rule 16). Whereas Rule 16 requires production to a defendant (after request) of information that is material to preparing the defense, Sanchez requests access to the ELSUR devices to examine the metadata "in order to determine whether recordings have been altered or deleted or whether additional recordings exist that have not been

disclosed. This meta data will also assist in determining the time and length of the recordings and the order in which they were created." Sanchez MTC at 13.

Thus, Sanchez requests the ELSUR devices' metadata and shows that it will be "material to preparing the defense," Fed. R. Crim. P. 16(a)(1)(E), in three ways: (1) determination whether the recordings have been altered or deleted; (2) whether additional recordings exist that have not been disclosed; and (3) determination of the time and length of the recordings and the order in which they were created. Under Rule 16 and this Court's previous Memorandum Opinion and Order in *DeLeon*, 2017 WL 2271430, at *48, Sanchez established that the metadata is material to preparation of his defense, and is thus entitled to the metadata.

B. THE UNITED STATES ALREADY PRODUCED TO SANCHEZ (AND THE OTHER DEFENDANTS) THE ELSUR DEVICES' METADATA.

The United States already provided to Sanchez and the remaining Defendants the ELSUR recording devices' metadata in June 2017. So Sanchez has all of the materials or information that form the basis of his request for access to the ELSUR recording devices.

But, at the November 9 and November 27 motions hearings, the United States failed to make a clear record that the evidentiary DVDs provided to the Defendants, which include the metadata, contain all of the helpful information that Sanchez requested in his Sanchez MTC.

With regard to Sanchez's first contention: that he needs access to the ELSUR recording devices, because "examination of the metadata is necessary in order to determine whether recordings have been altered or deleted," Sanchez MTC at 13, he has access to all of the metadata that was contained on the devices. The United States anticipates that Sup. SA Williamson will explain that the multi-layer protection systems in place with the ADS recording devices ensure that no recording sessions have been altered or deleted. And the Defendants possess the metadata that can verify Sup. SA Williamson's testimony. They may verify his

testimony that by seeing that the Bird software doesn't display "CHECKSUM ERROR" when they play the recording sessions. *See* Mathe ADS Declaration. The second way in which the Defendants may verify the integrity of the recording sessions is with the hash values that are included in the metadata in separate files on the evidentiary DVDs.

With regard to Sanchez's second contention: that he needs access to the ELSUR recording devices, because "examination of the metadata is necessary in order to determine . . . whether additional recordings exist that have not been disclosed," Sanchez MTC at 13, Sup. SA Williamson will explain that, given the nature of the multi-layer protection system ADS created for its body recorders, including the ELSUR procedure through which the devices are downloaded, an evidentiary DVD such as those produced to Defendants cannot exist unless it contains every single piece of data (and metadata) that was on the ELSUR device when downloaded -- in exactly the same form in which that data was generated when it was generated. Just as the ADS software generates an error message when it attempts to play a recording session for which the hash values do not align under its algorithm, the ADS download system through the standalone computer will not complete the download unless all of the data (and metadata) is downloaded completely to the evidentiary DVD. Thus, because the evidentiary DVDs which were produced to Defendants exist, there is no question that additional recording sessions did not exist which were not produced to Defendants. (In other words, the DVDs in Defendants' possession contain everything that was ever created on the ELSUR recording devices from when they were deployed with the CHSs to when they were given to the ELSUR Operations Technician to download onto the evidentiary DVDs.)

Finally, with regard to Sanchez's third contention: that he needs access to the ELSUR recording devices, because the metadata "will also assist in determining the time and length of

the recordings and the order in which they were created," Sanchez MTC at 13, that metadata is contained in the DVDs given to the Defendants, and the time and length of the recording sessions to the extent that it exists is viewable when playing the recording sessions through the Bird software.

Now, the United States qualified this answer with the qualifier that the Defendants have this information and may view it "to the extent that it exists," because this answer is a bit more nuanced. The United States identified three evidentiary DVDs in which the time that the Bird software reflects that the recording was taken is inaccurate. And on one of these three DVDs, the length of the recording sessions is also inaccurate, as it shows that the recordings are 0 minutes and 0 seconds long. The errors on this DVD of the session timing information is easily discovered by simply playing the recordings. For these 3 evidentiary DVDs, the times (and, on the one DVD, the session lengths) accurately reflect the metadata that was contained on the ELSUR device when the recording sessions were created. The hash values assigned when the recordings were created on the device and those assigned when the data was transferred to the evidentiary DVD align and are accurate. That accurate reflection of the data is why the ADS software allowed the evidentiary DVD to be created without displaying an error message, and is why the Bird software allows the recordings to be played without displaying the error. The inaccuracies aren't because of any type of manipulation or malfunction in the data created.

Thus, the United States produced to Defendants all of the information and materials in the United States' possession that may be material in preparing the Defendants' defense. The United States, therefore, complied with its Rule 16, as well as with its *Brady* and *Giglio*, obligations. Neither Rule 16, *Brady*, nor *Gilgio* support further disclosure of information or materials, including allowing Defendants, or even a single Defendant's attorney and that

attorney's forensic computer expert, to access the ELSUR devices used in this case or a similar device. The Court should therefore reconsider its order to disclose, and conclude that such disclosure is not necessary or proper.

C. THE DEFENDANTS ALREADY HAVE, OR BY THE END OF THE HEARING ON THIS MOTION WILL HAVE, ALL OF THE PROBATIVE INFORMATION THAT THEY SEEK IN ASKING FOR ACCESS TO THE ELSUR RECORDING DEVICES.

Aside from the reasons for access that Sanchez articulated in his Sanchez MTC, Defendants asked for disclosure of the ELSUR recording devices on the basis that the United States was unable to explain at the hearings why, precisely, there were gaps of time between two recording sessions. Defendants asked for disclosure to their forensic computer expert to "verify" the United States' counsel's representations that no data (or metadata) remained on the ELSUR devices. And Defendants asked for disclosure of the devices on the basis that: What is the concern in limited disclosure to an attorney and computer forensic expert if the United States is willing to allow convicted felons possess the devices without supervision in their prison cells? The United States is able to provide the information and answers that Defendants seek, and the Court should therefore reconsider its limited order of disclosure and conclude that Defendants are not entitled to access the ELSUR recording devices.

First, the United States is able to account for all of the time associated with the use of the ELSUR recording devices -- there are no gaps. What Defendants refer to as "gaps" between the recording sessions aren't gaps, but are due either to the CHS/user turning "OFF" and back "ON" the recording device, or because of operations internal to the ADS ELSUR recording device. The United States is also able to help Defendants ascertain the cause of gaps that they see in the Bird software. And the United States will present Sup. SA Williamson's testimony to explain these gaps. For instance, in the recording sessions of Defendant Rudy Perez that were used as

examples in court on November 9, 2017, the Court noticed that there was a gap of a few seconds between the first session and the second, and a gap of 19 minutes between the second and third recording session. These gaps were created by the CHS operator of the ELSUR recording device turning "OFF" and then back "ON" the recording device. That is established because there is no alert flag that appears next to the session number on the Bird software. With no alert flag apparent, that establishes that the CHS turned off the recording device manually to end the first session, and turned it back on manually a few second later to begin the second session. Similarly, the CHS turned off the device manually to end the second session, and turned it back on 19 minutes later to initiate the third session.

If something internal to the ELSUR recording device -- as opposed to the CHS-user -- had caused a recording session to end, then that will be reflected in the Bird software with an alert flag in the column next to the session number. Depending on the color of the flag, it establishes that the device either malfunctioned in some manner (*i.e.*, the battery went dead, or the memory on the device ran out), or that the data file was too large and the recording was split into multiple sessions by the software. (The meanings of a flag's color may be found by pulling down the help menu at the top of the Bird software player and clicking on "Flags Description").

Those are the only ways in which separate recording sessions are created.

Second, production of the ELSUR recording devices would not allow the Defendant's attorney or the Defendant's attorney's computer forensic expert to verify, beyond what the expert will see on the evidentiary DVDs already produced, that no data (or metadata) exists on the ELSUR recording devices once the devices are downloaded by the ELSUR Operations Technician to the evidentiary optical drive or disc (and then wiped clean). Sanchez stated at the hearing that the Court should allow his forensic computer expert access to the ELSUR recording

devices used in this case because he believes his expert can "see what's on the hard drive" or whatever "electronic data is that you can't access through a software program." Tr. at 14:4-13 (Jacks). But his forensic computer expert cannot examine what's on these ELSUR recording devices. Indeed, even the FBI cannot examine what's on these ELSUR recording devices. Only ASI, the company that manufactures the devices, and that writes and edits the software, can examine what data is on the ELSUR recording devices. As ASI President Mathe writes avers in the attached Declaration: "ADS . . . controls the opportunity to alter the recordings because the recorder may only be accessed using ADS proprietary software. The ADS software limits user [*e.g.*, FBI] actions to 1. changing performance settings; 2. download, 3. playback/viewing/ creation of user copies, and 4. erasure of the data on the recorder." Mathe ADS Declaration. Thus, Defendants' attorneys' computer forensic experts cannot "in fact, verify the representations that were just made by Mr. Castellano." Tr. at 15:18-23 (Jacks). But Defendants' attorneys' computer forensic experts can verify, beyond, the United States' counsel's representations (which the United States anticipates Sup. SA Williamson will testify at the hearing). They may analyze all of the metadata from the ELSUR recording devices, which is contained on the DVDs provided to the Defendants. The Court should therefore reconsider its order to produce, and conclude that production is not necessary or proper.

But even if Defendants' computer experts couldn't verify these representations and testimony by viewing the data on the DVDs provided, which they can, that is not a sound legal basis for production under Rule 16, *Brady* or *Giglio*. *See DeLeon*, 2017 WL 2271430, at *45-50. Asking to verify uncontroverted testimony doesn't meet this Court's requirement that "[t]he Defendants will have to make the necessary showing" that Rule 16, *Brady*, or *Giglio* entitles them to production of the information sought. *Id.* at *48. Verification alone, without some

indication that the requested relief will provide the probative information sought, is the quintessential fishing expedition, and is not a proper basis to be provided access to the law-enforcement-sensitive ELSUR recording devices over the United States' assertion of its privilege. Defendants have not made that "necessary showing" here, *id.*, because the information on the evidentiary DVDs they possess have all of the information (data, including metadata) that the United States possessed at any time for any of the ELSUR recording devices used. Once they hear from Sup. SA Williamson about the operations of those recording devices, then Defendants will have all of the information probative to preparing their defense, including information to impeach the CHSs and frame for the jury the weight they believe the jury should give to the recordings. Otherwise, given that Defendants have all of the information that may be helpful to preparing their defense, they cannot demonstrate that "there is a 'compelling need' for the information" relevant to the party's case. *In re City of New York*, 607 F.3d at 948 (quoting *Friedman*, 738 F.2d at 1343). Defendants have not, therefore, overcome the additional hurdles necessary to overcome the law-enforcement-sensitive qualified evidentiary privilege that the United States asserts in relation to these ELSUR recording devices. *See id.* (to rebut the presumption against lifting the privilege, the party seeking disclosure must show: (1) the request is "non-frivolous and brought in good faith"; (2) "the information sought is [not] available through other discovery or from other sources"; and (3) there is a "compelling need" for the information relevant to the party's case (citation omitted)).

D. THE COURT SHOULD NOT, GIVEN THE LAW-ENFORCEMENT-SENSITIVE NATURE OF THE ELSUR RECORDING DEVICES, ORDER THE UNITED STATES TO PRODUCE THE DEVICE FOR INSPECTION.

The Defendants have not made the showing necessary to overcome the United States' law-enforcement-sensitive qualified privilege asserted with respect to the inspection of the

ELSUR recording devices. The Court properly should, therefore, reconsider its limited order of production, and not require the United States to produce such a device for inspection. The Court also should reconsider its order for three additional reasons. First, although perhaps effective, the argument that the Court should order production based on that there is some inconsistency or illogic to the United States' decision to provide the devices to the CHSs, whom are convicted felons, but not to attorneys and not to a computer forensic expert, does not find support in the law or the facts for the Court's order to produce the device. Second, an order to produce these ELSUR recording devices for inspection would be a matter of first impression, and would set a poor and dangerous precedent for future production, completely destroying the utility of this covert recording device and means in any future investigations. Third, such production would harm national security interests.

Defendants' contention that the United States' decision to conduct its investigation by providing law-enforcement-sensitive ELSUR recording devices to convicted felons, but not to consent to provide them to Defendants under a limited production, does not find support in the law or in the facts of this case for the Court's order of disclosure. The United States' decision to provide these law-enforcement-sensitive devices to CHSs who are convicted felons, and not to law-abiding attorneys and forensic computer experts who are subject to the Court's contempt powers, may seem unfair or illogical, but that's the United States' prerogative, including under the Rules of Criminal Procedure and the Constitution. That the United States' decision appears unfair or illogical is not a basis on which the Court may properly order disclosure of the law-enforcement-sensitive ELSUR devices. The United States properly may decide how it conducts its investigations. Sometimes that conduct isn't pretty; law enforcement officers or agents may mislead or misrepresent facts to suspects to elicit information. Sometime law enforcement may

use unsavory individuals to penetrate secretive criminal organizations. And oftentimes, the worse the individual's criminal history or wrap sheet, the more effective that individual is as a CHS. Under these circumstances, if providing law-enforcement-sensitive objects or methods to these criminals/CHSs destroyed the law-enforcement-sensitive qualified privilege, then that privilege wouldn't exist at all. That can't be correct.

Second, at the November 9, 2017 motions hearing, the Court pointed out that there was some "force" to Defendants' logical argument about what harm may come from providing these sensitive devices to Defendants' attorneys and their computer forensic experts when they've already provided them to CHSs not under constant supervision: "I don't quite understand it, because I do think what you saying has some force. They've got a bunch of these recording devices running around in prison. What is so secret now that we're in a court that I can't have one lawyer and one expert look at it?" Tr. at 17:5-9 (Court). The Court reiterated at the November 27, 2017 Motions Hearing that this argument was the basis of the Court's order of disclosure. *See* Nov. 27 Tr. 141:15-23 (Court).

This order of disclosure is improper for two reasons, beyond those that it doesn't include the factual findings and conclusions necessary to overcome the United States' assertion of the privilege. First, the FBI gave these devices to prisoners to take into the prisons, where the devices were contraband, and possession of these recording devices by a prisoner could get that prisoner killed. These CHSs in prison couldn't deliberately inspect the ELSUR recording devices. They had to hide them the entire time they had them. If the guards found them, they were contraband and the CHS prisoner would be reprimanded. And if another prisoner -- especially an SNM-member prisoner -- found that the CHS had a recording device that he used to record incriminating conversations, the CHS faced almost certain death. So it's not as if these

prisoners could reverse engineer these devices while they had them. Second, if the Court looks back questions it asked of the United States at the May 2017 hearing when these devices were first at issue, and questions it asked of the United States at the November 9 hearing, and at the November 27 and 29 hearings, each time the Court asked whether the United States/FBI has ever been ordered by any court to produce these devices in the past. Why ask that question? The answer is, if the answer to that question is yes -- the FBI has been ordered to produce these devices physically for inspection -- there's precedent and it takes away the sting of the Court's order here to produce these sensitive devices for the first time. In United States' counsel's discussions with the FBI OTD, in all of the litigation that the OTD attorneys have seen regarding these ELSUR recording devices or similar law-enforcement-sensitive body recorders, they have never had a court order production of any such device. As Sup. SA Williamson will explain, that's why ADS manufactures these devices and maintains complete control over the proprietary systems and software; there can't be any trace of possible manipulation of the data, or that trace of even *possible* manipulation may, in some instances, provide a basis for allowing defendants to physically inspect the devices. But as things stand now, these ELSUR recording devices have sound data recording integrity. They've never been subject to suppression of evidence. *See* Mathe ADS Declaration. After hearing from Sup. SA Williamson, this Court should reconsider its order of limited production, and conclude that there is no sound basis to order physical production of these devices.

At bottom, even the limited the production that the Court ordered could harm seriously national security interests. The material in this case that the United States is seeking to protect is of the type that the law-enforcement privilege envisioned -- information pertaining to law enforcement techniques and procedures, as well as information that would seriously impair the

ability of a law enforcement agency to conduct future investigations. *See In re The City of New York*, 607 F.3d at 944. *See also Winner*, 641 F.2d at 831; *Tuite*, 181 F.R.D. at 176-77; *Van Horn*, 789 F.2d at 1507-1508; *Dellwood Farms*, 128 F.3d at 1125 (7th Cir. 1997); *In re Dep't of Investigation*, 856 F.2d at 483-84.

Disclosing the precise methods and means of concealment and the locations of the ELSUR recording devices, or the specifications of such devices, unnecessarily compromises the sources and methods used and the future deployment of these investigative tools. Disclosure of methods used by the FBI to install or secret these audio recording devices could also cause unnecessary harm to future investigations where similar techniques may be used. The public's knowledge of such tradecraft and personnel could enable individuals to employ measures to evade such law enforcement actions.

For example, with specific knowledge of the technique used or the concealments, a criminal defendant, or other bad actors observing the trial, could defeat the purpose of the recording system. Allowing a Defendant's forensic computer expert to inspect the ELSUR recording device could lead to disclosure of sensitive law enforcement programs or even classified material. The United States is not questioning anyone's integrity. But these recording devices are sensitive. And information that may lead criminals to counterintelligence about these recording devices is lucrative. There is, therefore, a very large incentive to disclose such information, even at the possible threat of court sanctions, and even for persons who may have no intention of, or even entertain the idea of, disclosing such information otherwise.

These possibilities present an unacceptable risk, and squarely demonstrate how disclosure of the information "would be contrary to the public interest in the effective functioning of law enforcement," and it would compromise "the integrity of an enforcement technique" used, which

is the hallmark of the evidentiary privilege. *Tuite*, 181 F.R.D. at 176-77. Any compromise of the law enforcement sensitive information discussed herein will have a detrimental impact on the national security of the United States.

Moreover, even if the Court concludes that the Defendants meet their 3-prong burden to overcome the United States' proper assertion of privilege -- which they cannot meet -- the public interest in nondisclosure significantly outweighs defendant's need for the information. *See In re City of New York*, 607 F.3d at 945. The FBI has always asserted that its sources and methods, to include electronic surveillance capabilities and equipment are law-enforcement sensitive. And, importantly, FBI policy even dictates that the devices themselves are not to be compromised through court proceedings. So, in light of the national security interests that inhere in protection of these covert recording systems and methods, the public's interest in protecting this information clearly overcomes any limited probative value of any evidence concerning technical specifications of audio recording devices, specific training of government witnesses on sources and methods, tradecraft of entering and exiting defendant's residences during physical searches or installation of audio devices, and the identity and role of other non-testifying witnesses during collection activities. The Court should therefore reconsider, and withdraw, its order of limited physical production of the devices.

If the court requires further information or explanation on any matter contained within this motion, the government requests that the court hold an *ex parte* hearing so that the government may have the opportunity to provide further explanation regarding sensitive and/or classified matters.

CONCLUSION

The Defendants possess all of the information and data, including the metadata (and hashing) in existence that relates to the ELSUR device recordings. Nothing of evidentiary value will be gained by allowing the Defendants, their attorneys, or their computer forensics experts to inspect the ELSUR recording devices. Indeed, inspection of the recording devices may only serve to harm national security interests, by provided information that may be used for counterintelligence purposes. But Defendants cannot show that they have a compelling need for this information, or that they cannot obtain the probative information from other sources, because they will receive all of the probative information that they don't currently possess on the evidentiary DVDs through the testimony of Sup. SA Williamson. For these reasons, the United States respectfully requests that this Court reconsider its oral order for limited production of the ELSUR recording devices, and withdraw that order.

Respectfully submitted,

JAMES D. TIERNEY
Acting United States Attorney

Electronically filed on 12/6/17
MARIA Y. ARMIJO
RANDY M. CASTELLANO
MATTHEW M. BECK
Assistant United States Attorneys
200 N Church St.
Las Cruces, NM 88001
(575) 522-2304

I HEREBY CERTIFY that I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send electronic notification to defense counsel of record on this date.

/s/
MATTHEW M. BECK
Assistant United States Attorney